Georgia Senate Cybersecurity Meeting

Cyber Workforce Challenges

November 3, 2022

Georgia Cyber Center

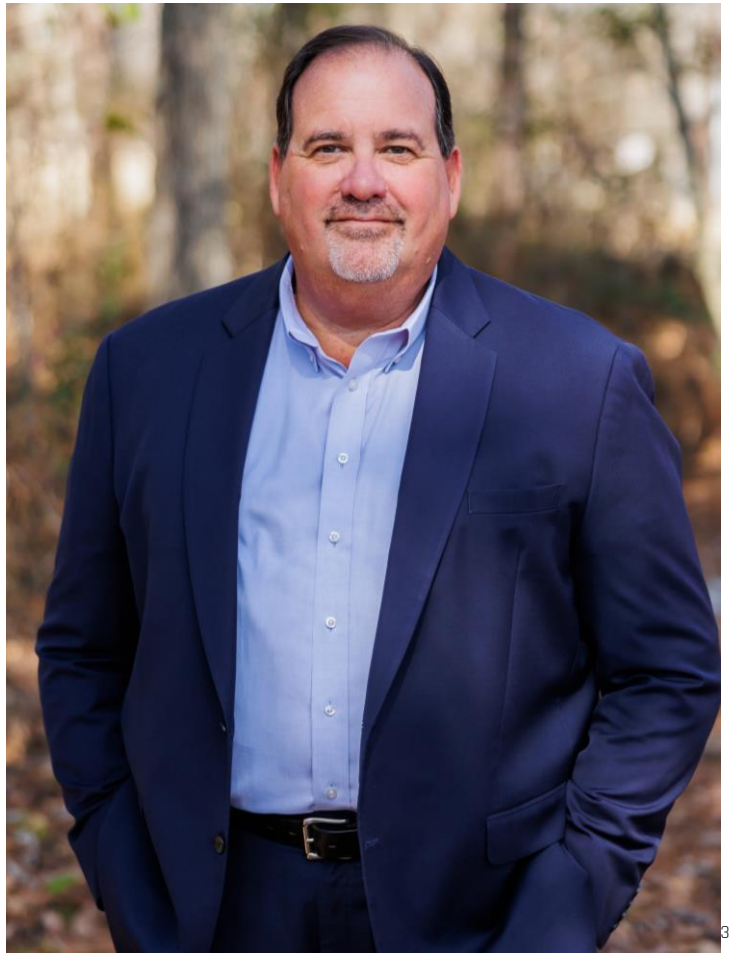
Timothy Kosiba, CEO

Bracket f, Inc.

Wholly-owned subsidiary of Redacted, Inc.
focusing on public sector markets

My background

Recently retired after 33 years of federal service; have led technical, forensic, offensive and defensive teams in the cybersecurity space for over 25 years



NSA

Deputy Commander of NSA Georgia
Chief of NSA's Tailored Access Operations (TAO)
Chief, Special US Liaison Officer - Canberra, Australia
Deputy Chief of NSA's Commercial Solutions Center (Private industry Liaison)

FBI

Directed the FBI Digital Forensic Laboratory – Computer Analysis Response Team

United States Navy

Naval Criminal Investigative Service

Education

BS, University of Baltimore, MIS
MS, George Washington University, Forensic Science

Today's Global Cyber Workforce Problem

The global cybersecurity workforce of 4.7 million people is still critically in need of more professionals. To adequately protect cross-industrial enterprises from increasingly complex modern threats, organizations are trying to fill the worldwide gap of 3.4 million cybersecurity workers.

At an enterprise level, the executive spotlight is pointed directly at cybersecurity teams, who are expected to adapt and protect their own organizations from mounting risks while complying with emerging technology and regulatory requirements.

The future of cybersecurity is defined by professionals evolving and persisting through the volatility of today's threat landscape. Traditional habits are being broken and diverse perspectives are entering the field, as the next generation uses new pathways to jump-start their careers.

https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

Today's National Cyber Workforce Problem

While the cyber workforce deficit constitutes a near- and long-term threat to our national and economic security, it also represents a significant opportunity to employ a more diverse and inclusive workforce in good-paying jobs that offer strong career possibilities

To help close the gap and maximize cyber-related employment opportunities, ensuring that cybersecurity training, education, and career pathways are available to everyone in our society with the passion and potential to do the work is necessary.

https://fcw.com/workforce/2022/10/white-house-seeks-advice-cyber-workforce-development/377995/

Why the urgency?

The need for extra cybersecurity staffing on top of an existing skills gap is putting organizations at significant risk. More than two-thirds (70%) of respondents reported that their organization does not have enough cybersecurity employees, with more than half arguing that staff deficits put their organization at a 'moderate' or 'extreme' risk of a cyber-attack.

Encouragingly, 72% of respondents expect their cybersecurity staff to increase somewhat or significantly within the next 12 months, which is higher than figures from the past two surveys (53% in 2021 and 41% in 2020). This follows the 11% rise in workers recorded this year. The fact the workforce grew by 11%, some 464,000 is cause for celebration. Adding nearly half a million people to the active workforce is a significant investment in cyber safety and defense.

While finding enough qualified talent was cited as the biggest cause for the shortage of cybersecurity staff (43%), the research showed there were numerous other internal factors organizations should work on to address the skills deficit.

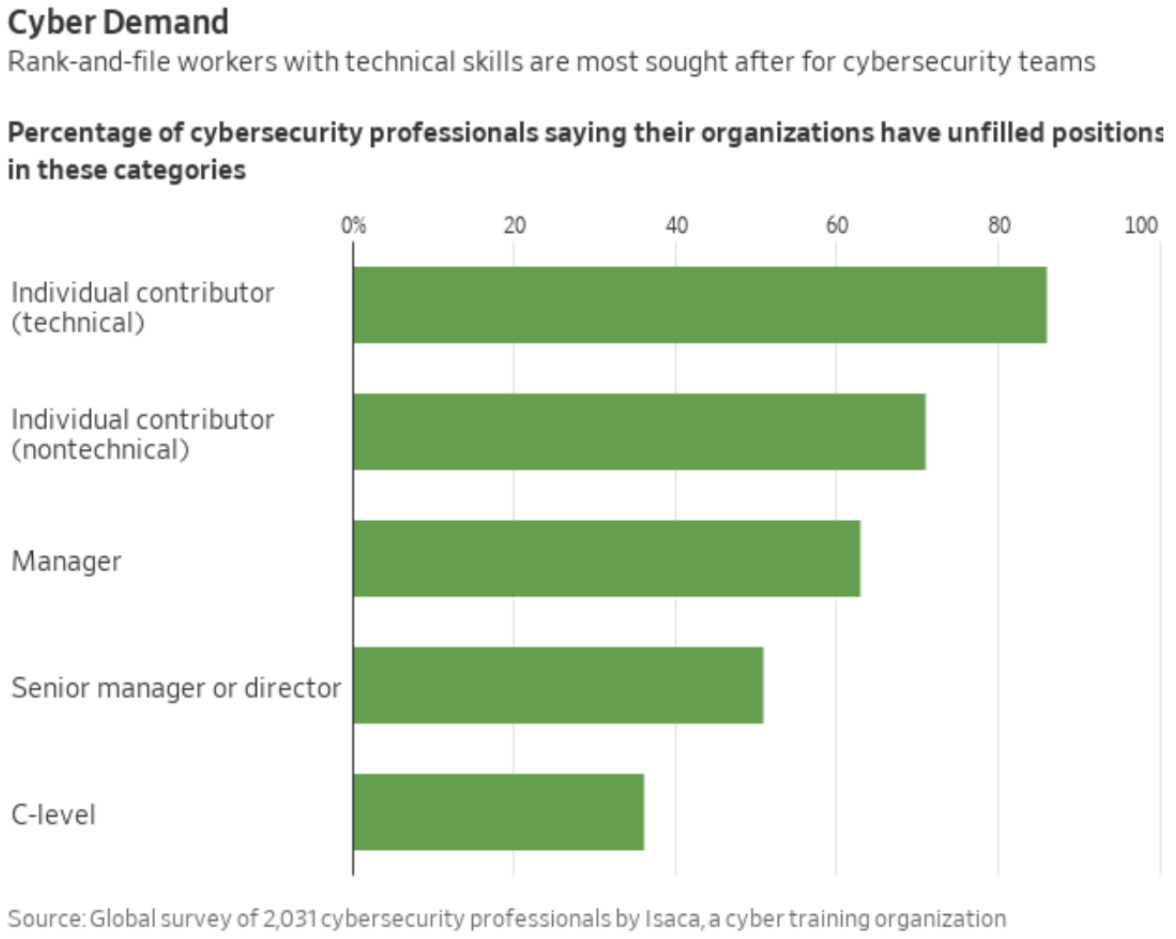
https://www.infosecurity-magazine.com/news/cybersecurity-workforce-gap-grows/

What skills are needed?

The biggest gap is in soft skills

"Respondents named a constellation of qualities they see lacking: flexibility, leadership, critical thinking, problem-solving, listening and speaking. While employers are trying to improve those skills with mentoring and online training, 17% of respondents said their organizations aren't doing anything about it, Isaca found."

Source: Wall Street Journal, Pro Cybersecurity newsletter, November 2, 2022



Impacts & Solution Space

While the cyber workforce deficit constitutes a near- and long-term threat to our national and economic security, it also represents a significant opportunity to employ a more diverse and inclusive workforce in good-paying jobs that offer strong career possibilities.

To help close the gap and maximize cyber-related employment opportunities, ensuring that cybersecurity training, education, and career pathways are available to everyone in our society with the passion and potential to do the work is necessary.

https://fcw.com/workforce/2022/10/white-house-seeks-advice-cyber-workforce-development/377995/

Impacts & Solution Space (cont'd)

Encouragingly, 72% of respondents expect their cybersecurity staff to increase somewhat or significantly within the next 12 months, which is higher than figures from the past two surveys (53% in 2021 and 41% in 2020). This follows the 11% rise in workers recorded this year. The fact the workforce grew by 11%, some 464,000 is cause for celebration. Adding nearly half a million people to the active workforce is a significant investment in cyber safety and defense.

While finding enough qualified talent was cited as the biggest cause for the shortage of cybersecurity staff (43%), the research showed there were numerous other internal factors organizations should work on to address the skills deficit (i.e., remote work, training & development opportunities, to name a few).

https://www.infosecurity-magazine.com/news/cybersecurity-workforce-gap-grows/

Impacts & Solution Space (cont'd)

Lastly, the State of Georgia has a wealth of talent and educational institutions to pull from, including the Georgia Cyber Center, Georgia Tech, University of North Georgia, University of Georgia, Augusta Tech, and many others.

Questions/Discussion

**Thank you to Senator Jason Anavitarte and Legislative Assistant Anna Horvath

